文章编号：2095-4980(2018)06-1072-08

基于矩阵的无线传感器网络 SNEP 改进

苏耀鑫，高秀峰

(陆军工程大学(石家庄校区) 信息工程系，河北 石家庄 050003)

摘　要： 针对网络安全加密协议(SNEP)存在过于依赖基站、密钥计算耗能大、密钥分发安全性较低的问题，采用了分簇式结构，引入矩阵与多密钥空间理论对 SNEP 进行改进。节点之间可利用加载的矩阵信息自主进行通信密钥计算。通过分析可知，该方案可降低基站依赖性，防范女巫攻击，并对基站的计算、存储需求降低，节点计算与存储开销没有明显增加，网络具有较高的安全性，可扩展性较好。

关键词： 无线传感器网络；网络安全加密协议；矩阵；多密钥空间

中图分类号： TN393　　**文献标志码：** A　　**doi：** 10.11805/TKYDA201806.1072

Research on improvement of SNEP protocol based on matrix

SU Yaoxin, GAO Xiufeng

(Department of Information Engineering, Ordnance Engineering College, Shijiazhuang Hebei 050003, China)

Abstract: Aiming at the existing problems of the Secure Network Encryption Protocol(SNEP) including that the protocol is too dependent on the base station, large energy consumption to calculate the key, the key distribution of low security, the network adopts the clustering structure, and introduces the matrix and the multi-key space theory to improve the SNEP. The calculation of the communication key can be carried out autonomously between the nodes using the loaded matrix information. Through the analysis, it is indicated that the program can reduce the base station dependency , prevent witch attacks, and decrease the calculation of the base station and storage requirements, also the node computing and storage overhead are not increased significantly; the network is of high security, and better scalability.

Keywords: wireless sensor network; Secure Network Encryption Protocol; matrix; multi-key space

无线传感器网络[1]由大量的能源有限，体积微小，价格低廉，具有数据监测及无线通信功能的传感器节点组成。节点在部署区域利用无线自组织的方式形成多跳的分布式网络系统，利用节点监测能力感知和收集监测区域的对象信息，采用数据传输及数据融合的方式将信息发送至用户。无线传感器网络因其独有的特点，成为热门的研究方向，已在很多方面得到广泛应用[2]，如智能家居、森林防火以及军事领域的情报监测等。与此同时，出现的安全问题[3]也受到了国内外许多机构及专家学者的关注。

无线传感器网络安全最重要且最基础的研究领域是以提供安全可靠的保密通信为目的的密钥管理方案[4]。近些年，专家和学者提出了许多关于无线传感器网络的密钥管理方案，如 Eschenauer 和 Gligor 首先提出的 E-G 方案[5]；为了进一步提高网络安全性，Chan,Perrig 和 Song 等在此基础上提出了 q-composite 方案[6]；Blundo 等提出的一种基于多项式的密钥预分配方案[7]；Blom 等提出了一种基于矩阵的密钥预分配方案[8]等。

各个国家的专家、学者致力于设计和研究高效的安全协议，使网络安全与协议相结合。目前国际上比较流行的安全协议有：链路层加密协议 TinySec[9]、轻量级安全协议 LEAP[10]、安全框架协议族 SPINS[11-12]。

1　网络安全加密协议(SNEP)简介

SNEP 是安全协议 SPINS 的 1 个子协议，是高效的通信协议。SNEP 采用数据加密以及消息认证码(Message Authentication Code，MAC)方式实现点到点的身份认证以及消息认证。

在 SNEP 中，若 2 节点需要协商通信密钥，则需要基站的参与，完成通信双方节点的身份确认以及通信密钥

收稿日期：2017-09-26；修回日期：2017-11-16

的计算和分发，节点间通信密钥的获取过程如图 1 所示。

节点 A,B,C,D,E 为普通节点，节点 A 申请与节点 B 通信，数据包内容如下：

1) N_A,ID_A

2) N_A,N_B,ID_A,ID_B,MAC{K_{AS},N_A,|N_B|IN_A|ID_B}

3) {SK_{AB}}K_{BS},MAC{K_{BS},N_A|ID_B|{SK_{AB}}K_{BS}}

4) {SK_{AB}}K_{AS},MAC{K_{AS},N_A|ID_B|{SK_{AB}}K_{AS}}

其中 N_A,N_B 表示节点 A,B 产生的随机数，防止恶意节点发起重发攻击；K_{AS},K_{BS} 分别表示节点 A,B 与基站共享的主密钥；ID_A,ID_B 表示节点 A,B 的身份标识；SK_{AB} 表示基站生成的身份认证密钥与消息认证密钥集合。

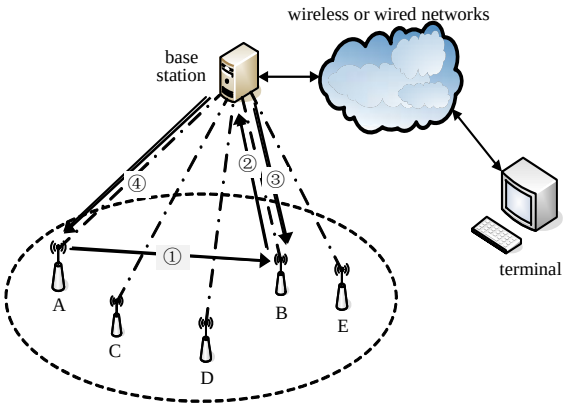


Fig.1 Key negotiation flow chart of the SNEP protocol

图 1 SNEP 协议密钥协商流程图

SNEP 存在许多特有的优势：a) 对通信的负担较小，只在每条消息的后面添加了部分位的数据；b) 使用了技术功能，避免了数据的传输，实现了语义安全，可以防止恶意节点的窃听；c) 能提供节点的身份认证功能，拥有重放保护，实现数据的机密性、新鲜性；d) 在传统预共享密钥技术的基础上，摒弃了任何 2 节点都共享密钥的方式，将传统网络中的可信密钥分配中心(Key Distribution Center，KDC)与无线传感器网络相结合，由基站担任可信密钥分配中心，只有 2 个节点在需要通信时才与基站协商通信密钥，改进了传统预共享密钥方法对节点资源要求过高的缺点等。

但协议本身也存在部分缺点：因为节点之间建立通信密钥均由基站进行密钥的计算以及分发，这个过程过分依赖基站，即使基站认为是绝对安全的。在通信过程中，节点的数目过于庞大，基站会成为通信瓶颈，并且基站很容易受到拒绝服务(Denial of Service，DoS)攻击。

针对上述问题，综合基于矩阵的密钥管理方案与 SNEP 的优点，提出一种基于矩阵的 SNEP 改进方案，减少基站的任务量和对基站的依赖性，普通节点采用矩阵的方法自主计算通信密钥，避免基站统一计算分发密钥带来的不安全性。

2　基于矩阵的 SNEP 改进方案

2.1 方案的总体设计

针对 SNEP 存在过于依赖基站、密钥计算耗能大、密钥分发安全性较低的问题，网络采用分簇式结构，引入矩阵与多密钥空间理论对 SNEP 进行改进。节点之间利用加载的矩阵信息自主进行通信密钥计算，簇头节点分担基站任务，基站统一管理簇头节点，故基站是一个“大簇头”。簇头节点以上级别的通信与簇范围内的通信方式类似，本文只阐述簇范围内的通信。该方案达到的效果是：降低基站依赖性、防范女巫攻击，并且对基站的计算、存储需求降低，节点计算与存储开销没有明显增加，网络具有较高的安全性，可扩展性较好。方案的总体设计框图如图 2 所示。

2.2 方案的详细设计

网络部署初始化阶段，由基站和簇头节点共同配合完成公钥矩阵和主密钥矩阵的生成，并构建多密钥空间，最终将矩阵信息加载到普通节点上。

2.2.1 网络部署初始化

1) 公钥矩阵的计算与生成过程

每个簇的公钥矩阵是利用簇头节点的 ID 信息作为矩阵的“种子”产生的。簇头节点将自己的 ID 信息作为产生范德蒙公共矩阵 $\boldsymbol{G}$ 的最小“种子”，根据每个簇内节点数目的不同设置参数 N(N 大于簇内节点数)，根据参数 N 产生公共矩阵的“种子”集合 Λ，$\Lambda=\{ID,ID+1,\cdots,ID+(N-1)\}$。其中范德蒙公钥矩阵 $\boldsymbol{G}$ 的构建方式如式(1)所示。矩阵中的所有元素属于有限域 $GF(q)$ (q 为一个大素数)。其中 m 的值由簇头节点产生的主密钥矩阵大小来决定。

$$\boldsymbol{G}=\begin{pmatrix} ID^0 & (ID+1)^0\cdots & (ID+(N-1))^0 \\ ID^1 & (ID+1)^1\cdots & (ID+(N-1))^1 \\ \vdots & \vdots & \vdots \\ ID^{m-1} & (ID+1)^{m-1}\cdots & (ID+(N-1))^{m-1} \end{pmatrix} \tag{1}$$

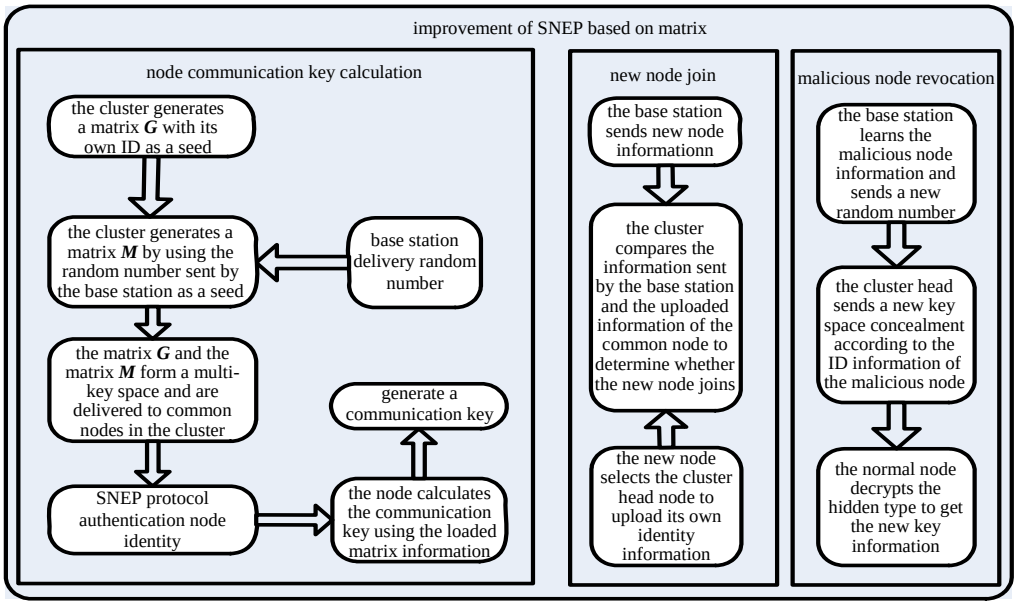


Fig.2 Improvement of SNEP based on matrix
图 2 基于矩阵的 SNEP 改进方案

2) 主密钥矩阵产生过程

主密钥矩阵由簇头节点根据基站下发的随机数产生。基站向每一个簇头下发一个数据集合 H，集合中包含基站产生的 q 个随机数，用于构建主密钥的“种子”集合，即 $H=\{F_1,F_2,\cdots,F_q\}$，其中每个“种子”构成一个 $m\times m$ 的对称矩阵，即主密钥 $\boldsymbol{M}_i(i\in(1,2,\cdots,q))$。

3) 密钥空间的建立

簇头节点将公钥矩阵 $\boldsymbol{G}$ 与主密钥 $\boldsymbol{M}_i(i\in(1,2,\cdots,q))$ 组合成为 q 个密钥空间 $\boldsymbol{S}_i=(\boldsymbol{G},\boldsymbol{M}_i)(i\in(1,2,\cdots,q))$，每个密钥空间拥有唯一的 ID。利用矩阵 $\boldsymbol{G}$ 与主密钥 $\boldsymbol{M}_i$ 计算私钥矩阵 $\boldsymbol{A}_i$，$\boldsymbol{A}_i=(\boldsymbol{M}_i\times\boldsymbol{G})^{\mathrm{T}}$。簇头节点选取 η 个密钥空间和私钥矩阵 $\boldsymbol{A}_i(i\in(1,2,\cdots,q))$ 加载到簇内普通节点内部。需要强调的是，并非是将密钥空间和私钥矩阵 $\boldsymbol{A}_i$ 的所有信息加载到节点内部，只需要将对应密钥空间的 ID、公钥矩阵 $\boldsymbol{G}$ 的第 i 列和私钥矩阵 $\boldsymbol{A}_i$ 的第 i 行加载到节点 i 上，减少节点存储资源的开销。

2.2.2 节点之间的密钥计算

1) 普通节点与簇头节点之间的密钥计算

SNEP 中，普通节点与基站之间的密钥由基站统一分发。本方案中所有的密钥采用矩阵理论，由节点自身计算，减小了簇头节点集中计算密钥造成的资源消耗。

簇头节点作为簇的一员，必须参与簇内节点之间的通信，以及与普通节点之间的通信密钥的协商过程。本方案中，簇头节点将公共密钥矩阵的第 1 列加载到自身，作为与簇内普通节点计算对密钥的公钥向量。普通节点利用自身存储的信息计算与簇头的通信密钥。由于簇头节点中存储所有主密钥 $\boldsymbol{M}_i$ 的信息，因此，普通节点从加载到自身的密钥空间中随机选择一个，并且选择与之对应的 $\boldsymbol{A}_i$ 的行向量，计算与簇头的通信密钥，如式(2)、式(3)所示。

$$K_{\mathrm{AH}}=[\mathrm{row}(1)\boldsymbol{A}_j^t\times ID^0]+\cdots+[\mathrm{row}(i)\boldsymbol{A}_j^t\times ID^1]+\cdots+[\mathrm{row}(m)\boldsymbol{A}_j^t\times ID^{m-1}] \tag{2}$$

$$K_{\mathrm{HA}}=[\mathrm{row}(1)\boldsymbol{A}_j^1\times(ID+(t-1)^0)]+\cdots+[\mathrm{row}(i)\boldsymbol{A}_j^1\times(ID+(t-1))^{i-1}]+\cdots+[\mathrm{row}(m)\boldsymbol{A}_j^1\times(ID+(t-1))^{m-1}] \tag{3}$$

式中：K_{AH} 为节点 A 计算的密钥；K_{HA} 为簇头节点计算的密钥；$\mathrm{row}(i)\boldsymbol{A}_j^t$ 为矩阵 $\boldsymbol{A}_j(j\in1,2,\cdots,q)$ 中第 t 行的第 i 个元素。由式(4)可得 K_{AH}=K_{HA}。

$$\boldsymbol{K}=\boldsymbol{AG}=(\boldsymbol{MG})^{\mathrm{T}}\boldsymbol{G}=\boldsymbol{G}^{\mathrm{T}}\boldsymbol{MG}=\boldsymbol{G}^{\mathrm{T}}((\boldsymbol{MG})^{\mathrm{T}})^{\mathrm{T}}=\boldsymbol{G}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}=(\boldsymbol{AG})^{\mathrm{T}}=\boldsymbol{K}^{\mathrm{T}} \tag{4}$$

2) 节点的身份认证

在 2 个节点进行密钥协商之前，利用簇头的作用进行节点之间的身份确认，可以提高网络的安全性。在 SNEP 中，由基站进行节点身份确认以及节点之间通信密钥的分发。在分簇的网络结构中，簇头节点分担基站的任务，代替基站对簇内节点进行身份确认和通信密钥分发。本方案中簇头节点舍弃向簇内节点分发密钥的任务，只进行

节点身份确认。节点通信密钥由节点自身利用矩阵信息计算得出。具体的身份确认流程如图 3 所示。

a) $N_A, ID_A, SID_A \oplus \boldsymbol{G}_A$

SID_A 表示节点 A 中加载的密钥空间的身份标识集合；$\boldsymbol{G}_A$ 是加载到节点 A 上的公钥矩阵 $\boldsymbol{G}$ 的列向量，节点 B 存储 $SID_A \oplus \boldsymbol{G}_A$ 值。

b) $SID_b, K_{BH}(N_A \| ID_A \| N_B \| ID_B \| SID_b)$

SID_b 是节点 B 在自身记载的密钥空间中随机选择的一个密钥空间的身份标识，并用此密钥空间计算出与簇头的通信密钥 K_{BH}。

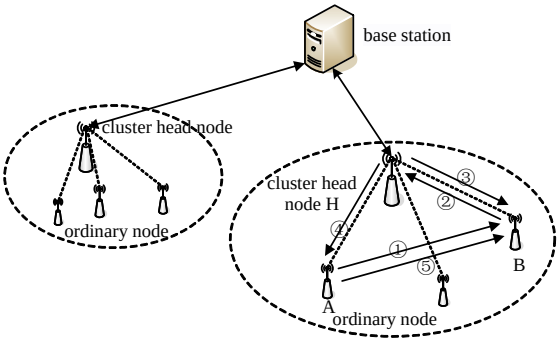


Fig.3 Flow chart of identity authentication
图 3 身份确认流程图

c) $N_B, K_{HB}(N_B \| T)$

簇头节点利用节点 B 发送的密钥空间身份标识计算与节点 B 的通信密钥 K_{HB}，簇头节点利用存储在自身的簇内节点列表判断节点的身份信息。其中 T 表示节点身份确认成功，反之，则为 F。

d) $SID_a, N_A, K_{HA}(N_A \| SID_a \| T)$

簇头节点从加载到节点 A 上的密钥空间中随机选择一个，身份标识为 SID_a，利用此密钥空间计算与节点 A 的通信密钥 K_{HA}。

e) $SID_B \oplus \boldsymbol{G}_B$

身份确认成功后，节点 B 将加载到自身的密钥空间身份标识集合和公共矩阵 $\boldsymbol{G}$ 的列向量发送至节点 A。

3) 节点之间的通信密钥计算

节点身份确认成功后进行节点间的通信密钥计算。由于每个节点加载多个密钥空间，节点根据自身加载的密钥空间 *ID* 信息与接收到的密钥空间 *ID* 信息进行比较，寻找相同的共享信息。如，节点 A 与节点 B 之间的共享密钥空间为 $\boldsymbol{S}_g$，则节点 A 根据 $\boldsymbol{S}_g$ 的信息计算通信密钥 K_{AB}，如式(5)所示。

$$K_{AB} = [\mathrm{row}(a)(\boldsymbol{A}_g)] \times [\mathrm{col}(b)(\boldsymbol{G})] \tag{5}$$

式中：$\mathrm{row}(a)(\boldsymbol{A}_g)$ 表示由密钥空间产生的私钥矩阵 $\boldsymbol{A}_g$ 的第 a 行，将其加载到节点 A 上；$\mathrm{col}(b)(\boldsymbol{G})$ 表示公钥矩阵 $\boldsymbol{G}$ 的第 b 列，将其加载到节点 B 上。同理可得 K_{BA} 计算如式(7)所示。

$$K_{BA} = [\mathrm{row}(b)(\boldsymbol{A}_g)] \times [\mathrm{col}(a)(\boldsymbol{G})] \tag{6}$$

由式(4)可知，K_{AB}=K_{BA}。

若节点 A 与节点 B 之间存在多个共享密钥空间，如共享密钥空间为 $(\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3)$，对其分别进行密钥计算，得出 $\left(K_{AB}^1, K_{AB}^2, K_{AB}^3\right)$，节点 A 使用 Hash 算法，计算 $K_{AB} = Hash(K_{AB}^1 \| K_{AB}^2 \| K_{AB}^3)$。

2.3 节点的加入与撤销

随着网络的运行，网络中的节点不断发生变化。节点会出现能量耗尽或者被俘获的情况，此时需要基站、簇头相互配合，将此类节点及时移出网络，否则会成为整个网络非常严重的安全隐患。节点的密钥更新可以有效地将老化节点和被俘节点移出网络。一个性能良好的网络必须要考虑网络的可扩展性，因此会出现新节点的加入，如何保证新加入的节点为安全节点是非常关键的问题。

2.3.1 新节点的加入

当新节点加入时，在部署之前，用户直接向基站发送数据包，告知新节点的相关信息。新节点向距离自身最近的簇头节点发送申请数据包，簇头节点将申请信息发送至基站，基站比较存储在自身的数据，判断是否吻合，进而决定是否同意新节点加入。具体流程如图 4 所示。

1) N_X, ID_X, K_{HX}

N_X 是用户产生的随机数；ID_X 是节点 X 的身份标识；K_{HX} 是由用户产生的用于簇头节点 H 与节点 X 交互的临时会话密钥，用于传输关于节点 X 的矩阵信息。用户将此数据包在部署之前加载到节点 X 上，并且发送至基站保存。

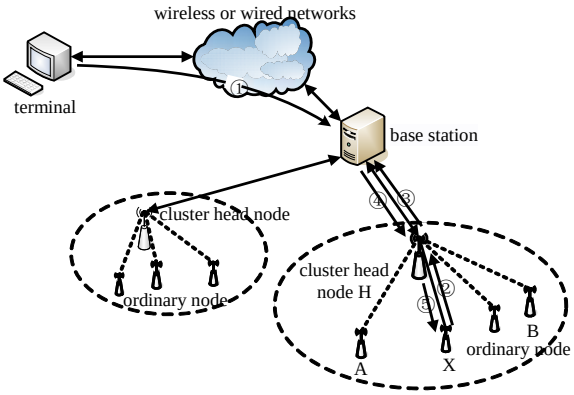


Fig.4 Flow chart of new nodes joining the network
图 4 新节点加入流程图

2) $N_{\mathrm{X}},ID_{\mathrm{X}},ID_{\mathrm{H}}$

节点 X 发送至簇头节点 H 的申请数据包。

3) $N_{\mathrm{X}},ID_{\mathrm{X}},N_{\mathrm{H}},ID_{\mathrm{H}}$

簇头节点 H 发送至基站的查询数据包。

4) $N_{\mathrm{X}},ID_{\mathrm{X}},N_{\mathrm{H}},ID_{\mathrm{H}},\{K_{\mathrm{HX}}\}K_{\mathrm{SH}}$

基站反馈到簇头节点 H 的数据包。$\{K_{\mathrm{HX}}\}K_{\mathrm{SH}}$ 表示基站 S 利用与簇头节点 H 间的通信密钥 K_{SH} 加密 K_{HX}。

5) $N_{\mathrm{X}},ID_{\mathrm{X}},\{\boldsymbol{G}_{\mathrm{X}}\,|\,\boldsymbol{S}_{\mathrm{X}}\}K_{\mathrm{HX}}$

簇头节点 H 将与节点 X 相关的矩阵信息用 K_{HX} 加密后发送至节点 X。其中，$\boldsymbol{G}_{\mathrm{X}}$ 表示加载到节点 X 上的公钥矩阵 $\boldsymbol{G}$ 的第 X 列向量；$\boldsymbol{S}_{\mathrm{X}}$ 表示加载至节点 X 上的多密钥空间集合信息。至此，新节点成功加入网络。

2.3.2 被俘节点的撤销

当节点的能量耗尽或者是节点被俘，要及时将此类节点移出网络。本方案采用更新密钥矩阵的方式，将非正常节点移出网络，实现网络的前向安全性。假设节点 Y 被俘获，则基站向节点 Y 所在簇的簇头下发被俘节点信息，以及新的生成主密钥矩阵的随机数集合 H'。簇头节点利用新的随机数集合产生新的主密钥矩阵 $\boldsymbol{M}_i'(i\in(1,2,\cdots,q))$。簇头节点向簇内广播 N' 个数据包，其中 N' 为当前簇内正常节点的数目。数据包的格式为：$K_{\mathrm{HZ}}(SID_{\mathrm{Z}}'\oplus\boldsymbol{A}_i'^{\mathrm{z}})i\in(1,2,\cdots,q)\quad Z\neq Y$。其中：Z 代表簇内的一个正常节点；$K_{\mathrm{HZ}}$ 是更新之前簇头节点与节点 Z 的通信密钥；SID_{Z}' 表示加载到节点 Z 上的新的密钥空间 ID 信息；$\boldsymbol{A}_i'^{\mathrm{z}}$ 为加载到节点 Z 上的新私钥矩阵 $\boldsymbol{A}_i'$ 的行向量集合。由于被俘节点 Y 与簇头节点的通信密钥 K_{YH} 无法解析任何一个数据包，因此无法获得新的密钥矩阵信息，被迫退出网络。其他的正常节点均可解析出一个数据包，获得新的密钥矩阵信息，网络继续正常运行。

3 方案分析

针对无线传感器网络的部署环境和节点结构的特殊性，对网络的安全性和网络性能进行分析。

3.1 安全性分析

本文在 SNEP 中引入矩阵和多密钥空间理论，采用分簇式的网络结构，节点间的密钥均采用矩阵理论计算。所以主密钥矩阵的安全性是方案整体安全性的关键。以此，从抵御主密钥攻击、女巫攻击以及拒绝服务攻击方面，分析方案的整体安全性。

3.1.1 抗主密钥攻击

在 Blom 方案中，存在安全阈值 λ，本文中 $\lambda=m$，如果网络中的 m 个节点被俘获，则这 m 个节点加载的公钥和私钥信息均暴露给攻击者，攻击者利用捕获的公私钥信息构建 m 个线性方程，主密钥矩阵 $\boldsymbol{M}$ 被破解。

本方案采用多密钥空间的方式，且网络结构为分簇式，簇内节点存储的密钥矩阵信息由基站产生的随机数生成，且簇间信息无相关性。

假设攻击者捕获了 m 个节点，且这 m 个节点同属于一个簇内，现需要破解其中一个主密钥 $\boldsymbol{M}_i\left(i\in(1,2,\cdots,q)\right)$，这 m 个节点中每个节点存储与主密钥 $\boldsymbol{M}_i$ 相关的私有矩阵 $\boldsymbol{A}_i\left(i\in(1,2,\cdots,q)\right)$ 的概率为 $p(1-p)^{\eta-1}$，其中 p 表示簇头节点从 q 个主密钥中选择 $\boldsymbol{M}_i\left(i\in(1,2,\cdots,q)\right)$ 的概率，故总概率为 $\left(p(1-p)^{\eta-1}\right)^m$。因为传感器节点所处环境较为复杂，捕获节点同属一个簇的可能性极小，故破获其中一个主密钥 $\boldsymbol{M}_i$ 的概率 $p_i<<\left(p(1-p)^{\eta-1}\right)^m$。反之，如果被捕获的 m 个节点中存在一个节点属于其他簇，则主密钥矩阵被破解的概率为零。

假设捕获的 m 个节点同属一个簇内，计算破解出主密钥矩阵 $\boldsymbol{M}_i\left(i\in(1,2,\cdots,q)\right)$ 的概率，如表 1 所示，通过设置不同的 m,q,η 得出破解概率 p_i 的值。

表 1 数据反映了簇内节点较少以及主密钥矩阵维度较小的情况，实际应用中网络规模远大于此，破解出主密钥矩阵 $\boldsymbol{M}_i\left(i\in(1,2,\cdots,q)\right)$ 的概率会更

表 1 抵御主密钥攻击的数据表

Table 1 Data table against master key attacks

η	q	m		
		3	4	5
3	5	$2.684\,4\times10^{-4}$	$3.436\,0\times10^{-5}$	$4.398\,0\times10^{-6}$
	6	$1.794\,5\times10^{-4}$	$2.077\,0\times10^{-5}$	$2.403\,9\times10^{-6}$
	7	$1.213\,5\times10^{-4}$	$1.273\,6\times10^{-5}$	$1.336\,8\times10^{-6}$
4	6	$8.654\,1\times10^{-5}$	$8.346\,9\times10^{-6}$	$8.050\,6\times10^{-7}$
	7	$6.440\,1\times10^{-5}$	$5.892\,6\times10^{-6}$	$5.301\,1\times10^{-7}$
	8	$4.917\,4\times10^{-5}$	$4.117\,9\times10^{-6}$	$3.448\,3\times10^{-7}$
5	7	$3.535\,6\times10^{-5}$	$2.726\,3\times10^{-6}$	$2.102\,3\times10^{-7}$
	8	$2.882\,5\times10^{-5}$	$2.112\,1\times10^{-6}$	$1.547\,4\times10^{-7}$
	9	$2.315\,2\times10^{-5}$	$1.606\,0\times10^{-6}$	$1.114\,0\times10^{-7}$

小。网络中的节点加载多个矩阵信息，对应多个主密钥矩阵，单独破解一个主密钥矩阵对网络的安全性影响较小。

3.1.2 抗女巫攻击

女巫攻击是指攻击者通过俘获节点得到相应的密钥信息，伪造一个非法节点，使其具有正常节点所具有的密钥形式，从而在网络中正常运行并且不被发现。它的基本过程为：攻击者将被捕获节点的公钥信息进行线性组合，编造出一个公钥 $\boldsymbol{G}_i$，如式(8)所示。

$$\boldsymbol{G}_i = \alpha_1\boldsymbol{G}_1 + \alpha_2\boldsymbol{G}_2 + \cdots\cdots + \alpha_{m'}\boldsymbol{G}_{m'} \tag{8}$$

式中 m' 表示被捕获节点的数量。

攻击者将被捕获节点的私钥信息进行线性组合，编造出一个私钥 $\boldsymbol{A}_i$，如式(9)所示。

$$\boldsymbol{A}_i = \boldsymbol{G}_i^{\mathrm{T}}\boldsymbol{M} = (\alpha_1\boldsymbol{G}_1 + \alpha_2\boldsymbol{G}_2 + \cdots\cdots + \alpha_{m'}\boldsymbol{G}_{m'})\boldsymbol{M} = \alpha_1\boldsymbol{A}_1 + \alpha_2\boldsymbol{A}_2 + \cdots\cdots + \alpha_{m'}\boldsymbol{A}_{m'} \tag{9}$$

攻击者通过配置 $\alpha_i\left(i \in (1,2,\cdots,m')\right)$ 的值来伪造非法节点的公钥与私钥信息。攻击者捕获一定数量的节点后，找出公钥与私钥的一一对应关系即可实现女巫攻击。如在 Blom 方案中，主密钥 $\boldsymbol{M}$ 与公共矩阵 $\boldsymbol{G}$ 均为单一存在，因此公钥与私钥的一一对应关系十分明显，抵御女巫攻击的能力非常有限。防范女巫攻击必须满足不能超过有 $m-1$ 个节点被捕获，即 $m' < m$。

多密钥空间、分簇的结合，使得节点的公钥与私钥的对应关系变得复杂，攻击者需要尝试和捕获更多的节点来实现攻击。在 Blom 方案中，假设攻击者最少捕获 μ 个节点可实现女巫攻击。现假设捕获节点数目相同的情况下，分析本方案实现女巫攻击的概率。

如果想要伪造一个节点，此节点需要存储 η 个主密钥构成的私钥矩阵相关信息，假设攻击者捕获了 μ 个节点，现计算攻击者捕获的 μ 个节点中存储的 $\boldsymbol{A}_i$ 信息对应主密钥 $\boldsymbol{M}_i$ 均相同的概率。选择其中一个节点为例，存储私钥矩阵 $\boldsymbol{A}_i\left(i \in (1,2,\cdots,q)\right)$ 的概率为 $P_1 = p(1-p)^{\eta-1}$，其中 $p = 1/q$，则存储下一个私钥矩阵 $\boldsymbol{A}_j\left(j \in (1,2,\cdots,q), j \neq i\right)$ 的概率为 $P_2 = p(1-p)^{\eta-2}$，其中 $p = 1/(q-1)$。以此类推，存储第 η 个私钥矩阵的概率为 $P_\eta = p$，其中 $p = 1/(q-\eta+1)$。就单个节点来说，存储与其他节点相同私钥矩阵的概率为 $P = P_1P_2\cdots P_\eta$，对于捕获的 μ 个节点，实现女巫攻击的总概率为 $P = (P_1P_2\cdots P_\eta)^\mu$。

通过设置主密钥个数以及每个节点的存储密钥数计算实现女巫攻击的概率值。如设置主密钥矩阵 m=5，则实现女巫攻击的概率值如表 2 所示。

表中的数据是在网络规模比较小、主密钥矩阵较简单的情况下发生女巫攻击的概率，实际应用中的节点数量远大于表中举例，因此实现女巫攻击的概率会更小，由此得出此方案抵御女巫攻击的能力较强。

表 2 实现女巫攻击的数据表

Table2 Data table against witch attacks

η	q	μ	
		4	5
3	4	$5.922\,4\times10^{-8}$	$9.239\,0\times10^{-10}$
	5	$4.096\,0\times10^{-9}$	$3.276\,8\times10^{-11}$
	6	$4.593\,9\times10^{-10}$	$2.059\,6\times10^{-12}$
4	5	$6.553\,6\times10^{-12}$	$1.048\,9\times10^{-14}$
	6	$3.544\,7\times10^{-13}$	$2.735\,1\times10^{-16}$
	7	$3.009\,1\times10^{-14}$	$1.253\,3\times10^{-17}$

3.1.3 抗 DoS 攻击

本方案借鉴基于矩阵的密钥管理方案对 SNEP 进行改进，实现节点的身份确认以及节点通信密钥的计算。基于矩阵的密钥管理方案和 SNEP 作用在平面网络结构中，具有一定的局限性。普通节点发送的密钥请求数据包，经过多跳的方式，到达基站后才进行处理。攻击者根据此特点发起 DoS 攻击，大量的虚假数据包汇聚到基站，导致合法数据包长期不被受理。本方案采用分簇的网络结构，一方面提高网络的可扩展性，另一方面可以减轻基站的通信流量，也易于将侵害范围控制在簇内。若恶意节点发送恶意通信申请数据包，簇头节点会首先对数据包进行身份验证，如果识别数据包为恶意数据包，则直接丢弃，避免出现恶意数据包一直传输到基站才被识别的情况，减少了通往基站的数据流量，有效抵御了恶意节点发起的 DoS 攻击。

3.2 网络性能分析

无线传感器网络节点部署环境的特殊性，决定了节点的资源开销和认证时延是衡量方案性能优劣的重要指标。通信、计算资源的消耗与节点的存储资源消耗密切相关，两者共同决定节点的能量消耗，最终关系网络的使用寿命。认证时延决定网络实现节点间通信的效率。

3.2.1 通信与计算开销

在无线传感器网络中，节点之间的无线通信开销要远大于计算开销。SNEP 中能量消耗分配情况如图 5 所示。摒弃 SNEP 由基站分配并计算和分发通信密钥的功能，只进行节点身份信息的确认。节点密钥由节点自身进行计算得出，减小了与簇头节点和基站通信带来的能量消耗。此过程中，普通节点计算通信密钥增加了节点的能量消耗，但这些能量消耗分散在各个普通节点，且计算复杂度低，较 SNEP 相比，缓解了能量在簇头节点的集中消耗，

延长了网络寿命。

SNEP 采用平面网络结构，如果网络的规模较大，则节点的 *ID* 与随机数 *N* 占用的空间位数将会增加。假设节点的 *ID* 为 2 Byte，随机数 *N* 为 4 Byte，基站向节点发送的通信密钥长度为 10 bit，则两节点进行一次密钥协商的通信开销为 356 bit。本方案采用分簇的网络结构，簇内节点数量远小于网络节点总数，节点 *ID* 长度仍为 2 Byte，但随机数长度减少为 2 Byte，密钥空间标识码为 1 Byte，则两节点进行一次密钥协商的通信开销为 208 bit，通信开销明显减小。普通节点计算通信密钥采用矩阵的行与列相乘，计算开销较低。

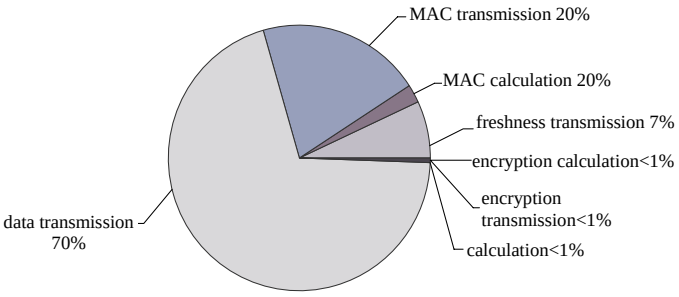


Fig.5 Distribution of energy consumption in SNEP
图 5 SNEP 协议的能量消耗分配图

3.2.2 存储开销

SNEP 中，普通节点存储与基站的主密钥，用于协商节点之间的通信密钥。Blom 方案中，节点存储的信息为 1 个列向量 $\boldsymbol{G}_i \in \boldsymbol{G}(i \in 1,2,\cdots,N')$ 和 1 个行向量 $\boldsymbol{A}_i \in \boldsymbol{A}(i \in 1,2,\cdots,m')$，$N'$ 为节点数量，m' 为主密钥矩阵的大小。本方案借鉴 Blom 方案改进 SNEP，并且采用多密钥空间方法，普通节点中存储的信息为 1 个列向量 $\boldsymbol{G}_i \in \boldsymbol{G}(i \in 1,2,\cdots,N)$、$\eta$ 个行向量 $\boldsymbol{A}_i^t \in \boldsymbol{A}^t\left(i \in 1,2,\cdots,m\right)\left(t \in 1,2,\cdots,q\right)$ 和 η 个密钥空间对应的 *ID* 信息 $SID_i\left(i \in 1,2,\cdots,q\right)$，其中 $\boldsymbol{A}^t$ 是由主密钥 $\boldsymbol{M}_t\left(t \in (1,2,\cdots,q)\right)$与公共矩阵 $\boldsymbol{G}$ 得出的私钥矩阵。和 SNEP 相比，存储开销虽有增加，但增加幅度较小，保持在节点存储允许的范围内，却较大幅度提高了网络节点通信安全性，故此代价是必要的。

3.2.3 认证时延

随着网络的运行，不断有合法节点向簇头节点发送节点认证请求数据包，在认证过程中伴随时延的产生。此类时延主要由 2 部分构成，分别是数据包在信道中传输产生的传输时延 t_{tm} 以及簇头和普通节点在密钥计算中产生的计算时延 t_{cl}。因此，节点认证时延的计算方法为：

$$t_{\mathrm{auth}} = N_1 t_{\mathrm{tm}} + N_2 t_{\mathrm{cl}} \tag{10}$$

式中：N_1 表示认证数据包所经过的跳数；N_2 表示请求认证的节点个数。将本文认证方案与 SNEP 以及基于非对称密钥的认证(Benenson 方案)过程进行模拟，并将各方案的认证时延进行对比，结果如图 6 所示。随着网络规模的增大，向簇头节点发送认证请求的节点个数增加，致使网络认证时延增大。基于分簇结构的网络扩展性较好，簇头节点分担基站部分认证任务，避免了大量数据包发送至基站造成消息碰撞，同时也减小了数据包转发跳数，降低了传输时延。因此，在相同认证请求节点个数下，本文方案与 Benenson 方案产生的认证时延高于 SNEP。此外，本方案是基于对称加密算法的身份认证，密钥计算复杂度较低，计算时延低于 Benenson 方案，因此认证时延略低于 Benenson 方案。

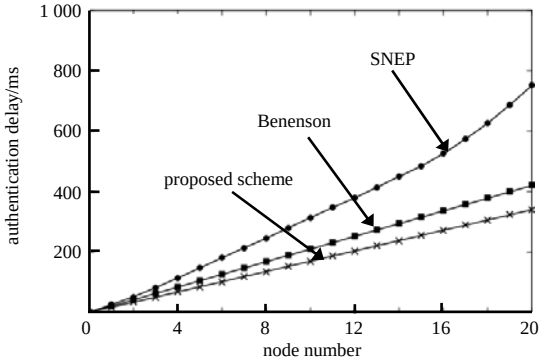


Fig.6 Comparison diagram of authentication delay
图 6 认证时延对比图

4 结论

本文在分簇式的网络结构中，将矩阵与多密钥空间的密钥管理方法与 SNEP 相结合，节点之间建立通信采用自主计算通信密钥的方式，减小了节点因集中计算密钥以及下发密钥产生的能量消耗。分析表明，开销处于网络允许的范围内，网络安全性有较大幅度的提高。

参考文献：

[1] 任丰原,黄海宁,林闯. 无线传感器网络[J]. 软件学报, 2003,14(7):1282−1291. (REN Fengyuan,HUANG Haining,LIN Chuang. Wireless sensor network[J]. Journal of Software, 2003,14(7):1282−1291.)

[2] SINGH D,TRIPATHI G,JARA A J. A survey of internet-of-things:future vision,architecture, challenges and services[C]// Internet of Things. Seoul,Korea:IEEE, 2014:287−292.

[3] 张玉泉. 无线传感器网络安全问题研究[M]. 济南:山东人民出版社, 2013. (ZHANG Yuquan. Research on wireless sensor network security[M]. Jinan,China:Shangdong People's Publisbing House, 2013.)

[4] MI Bo,CAO Jianqiu,DUAN Shukai,et al. Survey on key management of wireless sensor networks[J]. Computer Engineering and Applications, 2011,47(13):77–82.
[5] ESCHENAUER L,GLIGOR V D. A key management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. USA:[s.n.], 2002:41–47.
[6] CHAN H,PERRIG A,SONG D. Random key predistribution schemes for sensor networks[C]// Proceedings of IEEE Symposium on Security and Privacy. Berkeley,CA,USA:IEEE, 2003:197–213.
[7] BLUNDO C,SANTIS A D,HERZBERG A,et al. Perfectly secure key distribution for dynamic conferences[C]// Proceedings 12th Annual Int'l Cryptology Conf on Advances in Cryptology. New York,USA:[s.n.], 1992:471–486.
[8] BLOM R. An optimal class of symmetric key generation systems[C]// Proc. of Eurocrypt'84. Berlin,Heidelberg:[s.n.], 1984: 335–338.
[9] KARLOF C,SASTRY N,WAGNER D. TinySec:A link layer security architecture for wireless sensor networks[C]// Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems. Baltimore,US:[s.n.], 2004:162–175.
[10] ZHU Sencun,SETIA S,JAJODIA S. LEAP:efficient security mechanisms for large-scale distributed sensor networks[C]// Proceedings of the 10th ACM Conference on Computer and Communication Security. New York:ACM Press, 2003:62–72.
[11] PERRIG A,SZEWCZYK R,TYGAR J D,et al. SPINS:security protocols for sensor networks[J]. Wireless Networks, 2002,8(5): 521–534.
[12] 朱磊,吴灏,王清贤. 基于可信基站的 SPINS 协议研究与改进[J]. 计算机应用研究, 2010,27(6):2331–2334. (ZHU Lei, WU Hao,WANG Qingxian. Research and improvement of SPINS protocol based on trusted base station[J]. Application Research of Computers, 2010,27(6):2331–2334.)

作者简介：

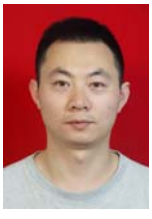
苏耀鑫(1993–)，男，甘肃省定西市人，在读硕士研究生，主要研究方向为网络对抗与信息安全.email:17310396927@163.com.

高秀峰(1973–)，男，石家庄市人，博士，副教授，主要研究方向为信息安全技术.

(上接第 1071 页)

[8] 张余,李连宝,柳永祥,等. 一种基于视意图式的用频系统电磁频谱参数泄露检测与识别方法[J]. 通信对抗, 2015,34(1): 11–14. (ZHANG Yu,LI Lianbao,LIU Yongxiang,et al. An electromagnetic spectrum parameters leaking detection and identification approach for spectrum-dependent systems based on view and sense marking schema[J]. Communication Countermeasures, 2015,34(1):11–14.)

作者简介：



张　余(1983–)，男，四川省邻水县人，硕士，副研究员，主要研究方向为电磁频谱技术等.email:zhyu63@163.com.

陈　勇(1975–)，男，湖南省衡阳市人，硕士，研究员，主要研究方向为电磁频谱技术、通信抗干扰技术等.

柳永祥(1985–)，男，武汉市人，硕士，高级工程师，主要研究方向为电磁频谱技术、通信抗干扰技术等.

罗明鉴(1983–)，男，四川省广元市人，硕士，工程师，主要研究方向为网电对抗等.